FEAC institute

Security Knowledge Framework: Integrating Information Security with the Enterprise Architecture

State of Maryland

Information Security and Privacy Conference 2004

Contact Information: Timothy Braithwaite
tim_braithwaite8@msn.com

Statement of the Problem

- Only rarely have contemporary computer-based information systems been designed with security (*ie. integrity, confidentiality, & availability*) in mind.
- More often, security is an afterthought with incompatible "point-solutions" being tacked onto already functioning "stovepipe" systems.
- Security integration of systems has become an underlying goal of recent IT legislation and OMB rulemaking – Sarbanes-Oxley for example!

Statement of the Problem

- The events of 9/11 and subsequent government organizational responses is accelerating the demise of “smokestack” systems in the name of information sharing.
- Creation of an Enterprise Architecture (EA) is viewed as an essential step in the development of systems capable of rapid and cost-effective information sharing. Given the current climate, these systems must be secure.
- Therefore, EA methodologies must accommodate information about security threats, requirements, and operating solutions as integral to the overall effort of “enterprise” systems development & subsequent modification.

Statement of the Problem

- Additionally, in order to *maintain* enterprise-wide information security, a “knowledge-base” of system security requirements and implementing hardware, software, and manual process “artifacts”must be established and managed for change.

- Finally, since nearly all previous IT security efforts have been undercapitalized, significant future progress will be made only when improved security ROI metrics can be devised.

What Is Needed?

- A methodology, compatible with prevailing EA methods and tools, is needed to elicit security-pertinent information about data, processes, connectivity, the organization, and key system development “artifacts”.

- Such a methodology can audit the “as is” system, describe the “to be” system, and be used as “base-line” documentation of security and integrity controls for Certification and Accreditation (C&A) and on-going change management purposes.

The Security Knowledge Framework (SKF) for Managing Enterprise-Wide Information Systems Security

- A methodology for identifying the knowledge needed to establish and continuously administer an effective program of information systems security across an enterprise.
- A model that assists with the visualization and assembly of the vast amounts of business and systems information and developmental "artifacts" needed to manage security in a cost-effective manner.
- A model that focuses attention on the critical "value issues" associated with information technology systems; thereby easing the challenge of determining a justifying Security ROI.
- Compatible with the pioneering EA work of John Zachman.

The Security Knowledge Framework

- Participants in SKF use:
  - Business Managers and System Users
  - Consumer Interest Groups
  - Designers/Programmers/Integrators
  - IG/Auditor/Legal
  - Computer Security
  - Quality Assurance

The Security Knowledge Framework

- What is Included?
- How the Framework supplements an on-going EA Initiative.
- How the Framework supports security certification and accreditation (C&A).

Security Knowledge Framework — Figure 1

	Data	Processes	Connectivity	Organization	Timing	External Requirements/ Constraints	Other Issues
Business Scope:							
Business Model							
Information Systems Model							
Technical Model							
Technical Definition							
Physical System Components							

Security Knowledge Framework — Figure 2

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Business Scope: (A)						• Business goals & objectives • Enterprise business plan • Economic analysis • IT plan • Security & privacy regulations • Audit standards • HR rulings	
Business Model (B)						Standards: • De-facto • ISO • Business Rules • Personnel policies • Security policies • Audit Reports Industry Threat Analysis	
Information Systems Model (C)						• Technology • Stability of basic technology • Availability of skilled personnel Application Risk Analysis	

Security Knowledge Framework — Figure 2 (Cont.)

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Technical Model (D)						• Data center security • Facilities security • Computer security practices/profile Application System Risk Analysis	
Technical Definition (E)						• Security software • DBMS controls • Vendor & outsource contracts • Backup agreement COTS & Contractor Risk Assessment	
Physical System Components (F)						• Security code in applications • IDS limitations • Backup & enforcement • Data destruction • Audit trails Change Management Continuity Plan	

Security Knowledge Framework — Figure 3

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Business Scope: (A)							Role supporting National Critical Infrastructure Participation in industry ISACs
Business Model (B)							Emerging legal requirements Pending legislation and regulations Evolving "due diligence" standards
Information Systems Model (C)							Evolving "best practices" for IT systems management

Security Knowledge Framework — Figure 3 (Cont.)

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Technical Model (D)							Structured systems development enforced? System security "best practices"
Technical Definition (E)							SEI Level equal to criticality of system Testing standards equal to criticality of system
Physical System Components (F)							Common Criteria standards System security "best practices" Intrusion Detection SIGs CIRC membership

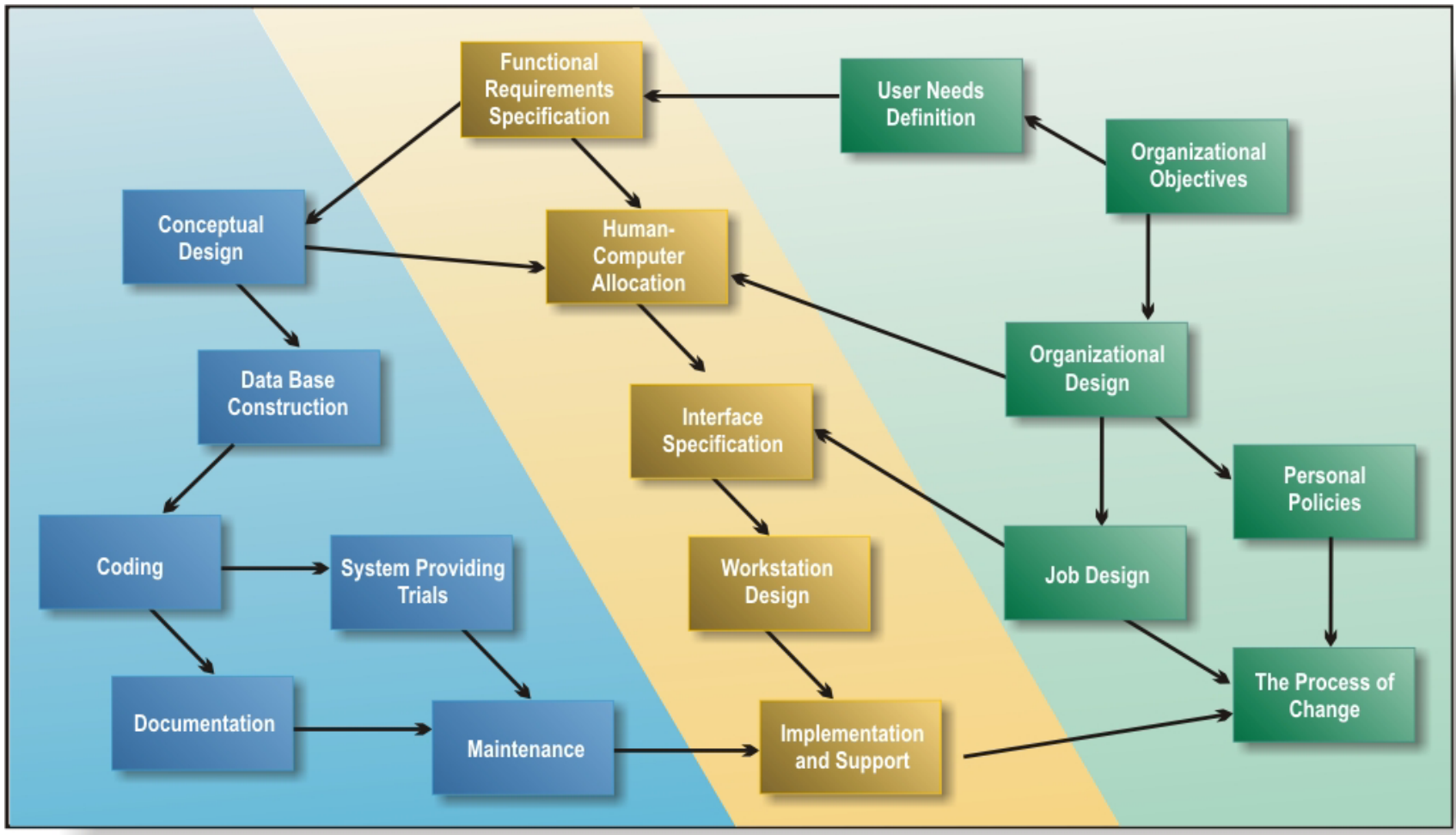
Security Knowledge Framework — Figure 4

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Business Scope: (A)	• Identify external & internal data needs • R&D data needs • Customer data and competitor data needs • Partner data needs • Value of strategic information to the Enterprise?					• Business goals & objectives • Enterprise Business Plan • IT Capital Investment Plan • Security & privacy regulations • Audit standards • HR rulings	Role supporting National Critical Infrastructure Participation in industry ISACs
Business Model (B)	• Data accuracy metrics • Data sensitivity • Classification schemes • Accounting rules • Auditing rules • Value of business data?					• Standards: • De-facto • ISO • Business Rules • Personnel policies • Security policies Audit Reports Industry Threat Analysis	Emerging legal requirements Pending legislation and regulations Evolving "due diligence" standards
Information Systems Model (C)	Quality factors: • Accuracy, etc. • Data relationships • Data exchanges • Data flows/views • Back-up demands • Test data - Value of having the Systems Model?					Technology: • Stability of basic technology • Availability of skilled personnel Application Risk Analysis	Evolving "best practices" for IT systems management

Security Knowledge Framework — Figure 4 (Cont.)

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Technical Model (D)	Logical System: • Elements & codes • Data base design • Edits & controls • Test data • Backups Value of accurate and timely data?					• Data center security profile • Facilities security • Computer security practices/profile Application System Risk Analysis	Structured systems development enforced? System security "best practices"
Technical Definition (E)	Physical Specs: • Edit routines • Correction routines • Check pt – restart, etc. • Backup routines Value of data documentation?					• Security software • -DBMS controls • Vendor & outsource contracts • Backup agreements COTS & Contractor Risk Assessment	SEI Level equal to criticality of system Testing standards equal to criticality of system
Physical System Components (F)	Physical System • Data structures • Access controls • Accuracy sampling • IDS criteria • Backups • Data recovery • Hot-Cold Sites • Firewalls Value of data Management hard/software?					• Security code in applications • IDS limitations • Backup & enforcement • Data destruction • Audit trails Change Management Continuity Plan	Common Criteria standards System security "best practices" Intrusion Detection SIGs CIRC member-ship

Elements Affecting the Design of a System for the Work Place — Figure 5



Security Knowledge Framework — Figure 6

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Business Scope: (A)	• Identify external & internal data needs • R&D data needs • Customer data and competitor data needs • Partner data needs Value of strategic information to the Enterprise?	• Business processes • Critical success factors • Interfaces • Supply chain nodes Value of unique business processes?				• Business goals & objectives • Enterprise Business Plan • IT Capital Investment Plan • Security & privacy regulations • Audit standards • HR rulings	Role supporting National Critical Infrastructure protection Participation in industry ISACs
Business Model (B)	• Data accuracy metrics • Data sensitivity • Classification schemes • Accounting rules • Auditing rules Value of business data?	• Data/information flows • Decision points • Inputs / outputs • Process criticality • Control objectives Value of knowing "How" a process works?				Standards: • De-facto • ISO Business Rules - Personnel policies • Security policies Audit Reports Industry Threat Analysis	Emerging legal requirements Pending legislation and regulations Evolving "due diligence" standards
Information Systems Model (C)	Quality factors: • Accuracy, etc. • Data relationships • Data exchanges • Data flows/views • Back-up demands • Test data Value of having the Systems Model?	Quality factors: • Integrity, availability, confidentiality, etc • Logical processes • Internal controls • Logical tests • Test data Value of process quality/integrity?				Technology - Stability of basic technology • Availability of skilled personnel Application Risk Analysis	Evolving "best practices" for IT systems.

Security Knowledge Framework — Figure 6 (Cont.)

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Technical Model (D)	Logical System: • Elements & codes • Data base design • Edits & controls • Test data • Backups Value of accurate and timely data?	• Logical System: • Processing specifications • Edit logic • Test logic • Test scenarios Value of processing integrity?				• Data center security profile • Facilities security • Computer security practices/profile Application System Risk Analysis	Structured systems development System security "best practices"
Technical Definition (E)	Physical Specs: • Edit routines • Correction routines • Check pt – restart, etc. • Backup routines Value of data documentation?	Physical Specs: • Program language statements • Test data statements • Read/Write/Delete, etc. matrix Value of process Documentation?				• Security software • DBMS controls • Vendor & outsource contracts • Backup agreements COTS & Contractor Risk Assessment	SEI Level equal to criticality of system Testing standards equal to criticality of system
Physical System Components (F)	Physical System : • Data structures • Access Controls • Accuracy sampling • IDS criteria • Backups • Data recovery • Hot-Cold Sites • Firewalls Value of data management hard/software?	Physical System • Executable code • Test programs • Change controls • Configuration management • IDS response • Checkpt restart & backups • Firewalls Value of process hard/software?				• Security code in applications • IDS limitations • Backup & enforcement • Data destruction • Audit trails Change Management Continuity Plan	Common Criteria standards System security "best practices" Intrusion Detection SIGs CIRC membership

Security Knowledge Framework — Figure 7

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Business Scope: (A)	• Identify external & internal data needs • R&D data needs • Customer data and competitor data needs • Partner data needs Value of strategic information to the Enterprise?	• Business processes • Critical success factors • Interfaces • Supply chain nodes Value of unique business processes?	• # of locations • Carriers • # of support vendors • CONUS • OCONUS • Internet Providers Value of connectivity to the Enterprise?			• Business goals & objectives • Enterprise Business Plan • IT Capital Investment Plan • Security & privacy regulations • Audit standards • HR rulings	Role with National Critical Infrastructure protection Participation in industry ISACs
Business Model (B)	• Data accuracy metrics • Data sensitivity • Classification schemes • Accounting rules • Auditing rules Value of business data?	• Data/information flows • Decision points • Inputs/outputs • Process criticality • Control objectives Value of knowing "How" a process works?	Type and Volumes: • Data • Voice • Mail • Courier • Encryption • Authentication Value of knowing "How" communi-cating works?			Standards: • De-facto • ISO • Business Rules • Personnel policies • Security policies Audit Reports Industry Threat Analysis	Emerging legal requirements Pending legislation and regulations Evolving "due diligence" standards
Information Systems Model (C)	Quality factors: • Accuracy, etc. • Data relationships • Data exchanges • Data flows/views • Test data Value of having the Systems Model?	Quality factors: • Integrity, availability, Confidentiality, etc. • Logical processes • Internal controls • Logical tests • Test data Value of process quality/ integrity?	Quality factors: • Accuracy, etc. • Volumes • Dedicated Line • Internet • VPN • Wireless Value of connectivity specifications?			Technology - Stability of basic technology • Availability of skilled personnel Application Risk Analysis	Evolving "best practices" for IT systems

Security Knowledge Framework — Figure 7 (Cont.)

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Technical Model (D)	Logical System: • Elements & codes • Data base design • Edits & controls • Test data • Backups Value of accurate and timely data?	• Logical System: • Processing specifications • Edit logic • Test logic • Test scenarios Value of processing integrity?	Logical System: • Network Model • LAN/WAN • Dial-up/mobile • Internet • Wireless Value of "wiring" Schematics?			• Data center security profile • Facilities security • Computer security practices/profile Application System Risk Analysis	Structured systems development System security "best practices"
Technical Definition (E)	Physical Specs: • Edit routines • Correction routines • Check pt – restart, etc. • Backup routines Value of data documentation?	Physical Specs: • Program language statements • Test data statements • Read/Write/Delete, etc. matrix Value of process documentation?	Physical Specs: • Host, • Nodes, • Routers, • Lines, • Internet Providers • Protocols • Public key (PKI) Value of network documentation?			• Security software • DBMS controls • Vendor & outsource contracts • Backup agreements COTS & Contractor Risk Assessment	SEI Level equal to criticality of system Testing standards equal to criticality of system
Physical System Components (F)	Physical System : • Data structures • Access controls • Accuracy sampling • IDS criteria • Backups • Data recovery • Hot-Cold Sites • Firewalls Value of data management hard/software?	Physical System • Executable code • Test programs • Change controls • Configuration management • IDS response plan • Checkpt restart & backups • Firewalls Value of process hard/software?	Physical System • Network controls • Capacity monitors • System backups • Public key software • Change control • Firewalls Value of all systems communicating across the Enterprise?			• Security code in applications • IDS limitations • Backup& enforcement • Data destruction • Audit trails Change Management Continuity Plan	Common Criteria standards System security "best practices" Intrusion Detection SIGs CIRC membership

Security Knowledge Framework — Figure 8

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Business Scope: (A)	• Identify external & internal data needs • R&D data needs • Customer data and competitor data needs • Partner data Value of strategic information to the Enterprise?	• Business processes • Critical success factors • Interfaces • Supply chain nodes • Value of unique business processes?	• # of locations • Carriers • Number of support vendors • CONUS • OCONUS • Internet Providers Value of connectivity to the Enterprise?	• Roles, responsibilities and authorities • Org charts • Locations • Supply chain members • Partners • Personnel policies • Security policies		• Business goals & objectives • Enterprise Business Plan • IT Capital Investment Plan • Security & privacy regulations • Audit standards • HR rulings	Role with National Critical Infrastructure protection Participation in industry ISACs
Business Model (B)	• Data accuracy metrics • Data sensitivity • Classification schemes • Accounting rules • Auditing rules Value of business data?	• Data/information flows • Decision points • Inputs/outputs • Process criticality • Control objectives Value of knowing "How" a process works?	Type and Volumes: • Data • Voice • Mail • Courier • Encryption • Authentication Value of knowing "How" to communicate?	Functions • What • Where • Authorizations • Work place structure • Need to know rules • Interfaces • Auditing rules		Standards: • De-facto • ISO Business Rules • Personnel policies • Security policies Industry Threat Analysis	Emerging legal requirements Pending legislation and regulations Evolving "due diligence" standards
Information Systems Model (C)	Quality factors: • Accuracy, etc. • Data relationships • Data exchanges • Data flows/views • Back-up demands • Test data Value of having the Systems Model?	Quality factors: • Integrity, availability, confidentiality, etc. • Logical processes • -Internal controls • Logical tests • Test data Value of process quality/integrity?	Quality factors: • Accuracy • Interoperability, etc. • Volumes • Dedicated Lines • Internet • VPN • Wireless Value of connectivity specifications?	Quality factors: • Privacy policies • Access policies • Separation of duties • User permissions – read/write, etc.		Technology -Stability of basic technology • Availability of skilled personnel Application Risk Analysis	Evolving "best practices" for IT systems

Security Knowledge Framework — Figure 8 (Cont.)

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Technical Model (D)	Logical System: - E lements & codes • Data base design • Edits & controls • Test data • Backups Value of accurate and timely data?	Logical System: • Processing specifications • Edit logic • Test logic • Test scenarios Value of processing integrity?	Logical System: • Network Model • LAN/WAN • Dial-up/mobile • Internet • Wireless Value of "wiring" schematics?	Organizational Structure: • Access model • Process access model • Permissions model • Audit trails		• Data center security profile • Facilities security • Computer security practices/profile Application System Risk Analysis	Structured systems development System security "best practices"
Technical Definition (E)	Physical Specs: • Edit routines • Correction routines • Check pt–restart, etc. • Backup routines Value of data documentation?	Physical Specs: • Program language statements • Test data statements • Read/Write/Delete, etc. matrix Value of process documentation?	Physical Specs: • Host, • Nodes, • Routers, • Lines, • Internet Providers • Protocols • Public key (PKI) Value of network documentation?	Physical Specs: • Access matrix • Permissions matrix: - Read, - Write, - Delete, - Append, etc. • Software Package Analysis		• Security software • DBMS controls • Vendor & outsource contracts • Backup agreements COTS & Contractor Risk Assessment	SEI Level equal to criticality of system Testing standards equal to criticality of system
Physical System Components (F)	Physical System • Data structures • Access controls • Accuracy sampling • IDS criteria • Backups • Data recovery • Hot-Cold Sites • Firewalls Value of data management hard/software?	Physical System • Executable code • Test programs • Change controls • Configuration management • IDS response plan • Checkpt restart & backups • Firewalls Value process hard/software?	Physical System • Network controls • Capacity Monitors • System backups • Public key software • Change controls • Firewalls Value of all systems communicating across the Enterprise?	Physical System • Password management • Network • Administration • Change control • Audit management • Incident Reporting/Response Procedures		• Security code in applications • IDS limitations • Backup& enforcement • Data destruction • Audit trails Change Management Continuity Plan	Common Criteria standards System security "best practices" Intrusion Detection SIGs CIRC membership

Security Knowledge Framework — Figure 9

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Business Scope: (A)	• Identify external data needs • R&D data needs • Customer data and competitor data needs • Partner data needs • Value of strategic information to the Enterprise?	• Business processes • Critical success factors • Interfaces • Supply chain nodes • Value of unique business processes?	• # of locations • Carriers • Number of support vendors • CONUS • OCONUS • Internet Providers - Value of connectivity to the Enterprise?	• Employees, roles responsibilities and authorities • Organizational charts • Office Locations • Supply chain members/vendors • Personnel policies • HR Security policies • Employee Unions	• Market fluctuations • Time to market estimates • Contract renewals • Patent/Renewals • Business cycle dependencies	• Business goals & objectives • Enterprise Business Plan • IT Capital Investment Plan • Security & Privacy Regulations • Audit Standards • HR rulings	Role supporting National Critical Infrastructure Participation in industry ISACs
Business Model (B)	-data accuracy metrics • Data sensitivity • Classification schemes • Accounting rules • Auditing rules • Value of business data?	• Data/information workflows • Decision points • Inputs/outputs • Process criticality • Control objectives • Value of knowing "How" a process works?	Type and Volumes • Data • Voice • Mail • Courier • Encryption • Authentication • Value of knowing "How" communi-cating works?	Functions - Who • Where • Authorizations • Work place location • Need- to- know rules • Interfaces • Audit Findings	Business Cycles: • Sales/Marketing • Product Development • Budget • Demand Cycles: • Triggers • Prompts • Queries	Standards: • De-facto • ISO Business Rules • Personnel Policies • Security Policies Audit Reports Industry Threat Analysis	Emerging legal requirements Pending legislation and regulations Evolving "due diligence" precedents
Information Systems Model (C)	Quality factors: • Accuracy, etc. • Data relationships • Data exchanges • Data flows/views • Back-up demands • Test data • Value of having the Systems Model?	Quality factors: • Integrity, availability, confidentiality, etc. • Logical processes • Internal controls • Logical tests • Test data • Value of process quality/integrity?	Quality factors: • Accuracy, etc. • Volumes • Dedicated Lines • Internet • VPN • Wireless • Value of connectivity specifications?	Quality factors: • Confidentiality policy • Access policy • Separation of duties • User permissions – read/write, delete, append, etc.	Quality factors: • Real-time defined • "as of" requirements • Timeliness • Turn-around • Through-put & volumes	Technology - Stability of basic technology • Availability of skilled personnel Application Risk Analysis	Evolving "best practices" for IT systems management

Security Knowledge Framework — Figure 9 (Cont.)

	Data (1)	Processes (2)	Connectivity (3)	Organization (4)	Timing (5)	External Requirements/ Constraints	Other Issues
Technical Model (D)	Logical System: • Elements & codes • Data base design • Edits & controls • Test data • Backups • Value of accurate and timely data?	Logical System: • Processing specifications • Edit logic • Test logic • Test scenarios • Value of processing integrity?	Logical System: • Network Model • LAN/WAN • Dial-up/mobile • Internet • Wireless • Value of "wiring" schematic?	Organizational Structure: • User access matrix • Software agent access matrix • Permissions matrix • Audit trail model	Logical System: • Response times • Turnaround limits • Service agreements • Downtime limits	• Data center security profile • Facilities security • Computer security practices/profile Application System Risk Analysis	Structured systems development enforced? System security "best practices"
Technical Definition (E)	Physical Specs: • Edit routines • Correction routines • Check pt–restart, etc. • Backup routines • Value of data documentation?	Physical Specs: • Program language statements • Test data statements • Read/Write/Delete, etc. matrix • Value of process documentation?	Physical Specs: • Host, • Nodes, • Routers, • Lines, • Internet Providers • Protocols • Public key (PKI) • Value of network documentation?	Physical Specs: • Access lists • Permissions list: - Read, - Write, - Delete, - Append • Access software vulnerabilities	Physical Specs: • Availability/reliability specifications • Downtime response • Maintenance response • Backups/Timing	• Security software • DBMS controls • Vendor & outsource contracts • Backup agreements COTS & Contractor Risk Assessment	SEI Level equal to criticality of system Testing practices equal to criticality of system
Physical System Components (F)	Physical System • Data structures • Access Controls • Accuracy Sampling • IDS criteria • Backups • Data recovery • Hot-Cold Sites • Firewalls • Value of data management hard/software?	Physical System • Executable code • Test programs • Change controls • Configuration management • IDS response plan • Checkpt restart & backups • Firewalls • Value of process hard/software?	Physical System • Network controls • Capacity Monitors • System backups • Public key software • Change controls • Firewalls • Value of all systems communicating across the Enterprise?	Physical System • Password management • Network administration • Change control • Audit management • Incident Reporting/Response Procedures	Physical System - Response time monitors • Auto-scheduling • Maintenance schedules • System recovery tests	• Security code in applications • IDS limitations • Backup& enforcement • Data destruction • Audit trail limits Change Management Continuity Plans	Common Criteria standards System security "best practices" Intrusion Detection SIGs CIRC membership